Research Paper | Law | E-ISSN No : 2454-9916 | Volume : 5 | Issue : 2 | Feb 2019

A STUDY ON INDIA'S CYBER LAW AND INFORMATION TECHNOLOGY ACT

Dr. Pankajkumar J. Modi

Assistant Professor, Government Law College, Maninagar, Ahmedabad, Gujarat, India.

ABSTRACT

IT is concerned with information systems, data storage, access, retrieval, analysis, and intelligent decision making. The term "information technology" refers to the generation, gathering, processing, storing, presenting, and disseminating of information, as well as the procedures and devices that make this possible. The misuse of technology has necessitated the establishment and implementation of cyber laws. Computers now play a significant role in practically every crime perpetrated. Citizens should not believe that cybercrime is on the decline, and they should understand that with each passing day, cyberspace becomes a more dangerous place to be in, where criminals wander freely to carry out their illegal intents, aided by the so-called anonymity that the internet affords. The paper focuses on new legislation that can encompass all aspects of cybercrime and should be approved in order to eliminate legal grey spots.

KEYWORDS: Cyber Law, Information Technology, Cyber Crime, Internet.

INTRODUCTION:

Recently, many information technology (IT) professionals lacked awareness of an interest in the cybercrime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy or at the least, distrust between the two most important players in any effective fight against cybercrime: law enforcement agencies and computer professionals. Yet close cooperation between the two is crucial if we are to control the cybercrime problem and make the Internet a safe "place" for its users.

Information is a resource which has no value until it is extracted, processed and utilized. Information technology deals with information system, data storage, access, retrieval, analysis and intelligent decision making. Information technology refers to the creation, gathering, processing, storage, presentation and dissemination of information and also the processes and devices that enable all this to be done.

Information technology is affecting us as individual and as a society. Information technology stands firmly on hardware and software of a computer and telecommunication infrastructure. But this is only one facet of the information Technology, today the other facets are the challenges for the whole world like cybercrimes and more over cyber terrorism. When Internet was first developed, the founding fathers hardly had any inkling that internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulations. With the emergence of the technology the misuse of the technology has also expanded to its optimum level.

The misuse of the technology has created the need of the enactment and implementation of the cyber laws. As the new millennium dawned, the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with the criminal element. According to Donn Parker , "For the first time in human history, computers and automated processes make it possible to possess, not just commit, a crime. Today, criminals can pass a complete crime in software from one to another, each improving or adapting it to his or her own needs." but whether this cyber laws are capable to control the cybercrime activities, the question requires the at most attention.

Until recently, many information technology (IT) professionals lacked awareness of and interest in the cybercrime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy or at the least, distrust between the two most important players in any effective fight against cybercrime: law enforcement agencies and computer professionals. Yet close cooperation between the two is crucial if we are to control the cybercrime problem and make the Internet a safe "place" for its users.

Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice. IT personnel understand computers and networks, how they work, and how to track down information on them. Each has half of the key to defeating the cybercriminal. IT professionals need good definitions of cybercrime in order to know when (and what) to report to police, but law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offense. The first step in specifically defining individual cybercrimes is to sort all the acts that can be considered cybercrimes into organized categories.

WHAT IS A COMPUTER CRIME?

- Criminals can use computer networks to operate anonymously.
- Privacy is being invaded by hackers.
- Computer Files or Records are used by hackers to destroy "property."
- By destroying information systems, hackers injure other computer users.
- Theft of Intellectual Property by Computer Pirates

CYBER OFFENDERS:

An offender or a criminal is someone who does something illegal with the goal of committing a crime. Any person who commits a Cyber Crime is referred to as a Cyber Criminal in this context. Children and teenagers aged 6 to 18 years may be cyber criminals; they may be organised hackers, professional hackers or crackers, disgruntled employees, cheats, or even psychics.

1. **Kids & Teenagers (age group 9-16 etc.):** Although it seems tough to believe, it is true. Teenagers make up the majority of amateur hackers and cyber criminals. Hacking into a computer system or a website is a source of pride for them, who have just recently began to comprehend what looks to be a great deal about computers. There's also the matter of appearing extremely intelligent among friends. These young rebels may also engage in cybercrime without being aware that they are doing so.

   Teen hackers, according to the BBC, have progressed from merely wanting to make a name for themselves to actually working their way into a life of crime through the use of computers. One of the most significant developments in 2004 was the decreasing impact of the boy hackers eager to make a name for themselves by designing a fast-spreading virus, according to Kevin Hogan. Although teen virus developers will continue to experiment with dangerous code, criminal use of malicious programmes increased significantly in 2004. The employment of technology by criminals was fueled by financial incentives.

   Another reason for the rise of teen offenders in cybercrime is that many offenders, mostly young college students, are uninformed of the seriousness of the crime. An engineering college student from Tamil Nadu was recently arrested by the Chennai city police for sending an unwanted mail to a chartered accountant. The young man has been released on bail. As a result, counselling sessions for college students must be initiated in order to educate

them on the seriousness of such crimes and the penalties that may result.

A Massachusetts teenager pled guilty in federal court in Boston in September 2005 for a spate of hacking offences that included the February penetration of online information broker Lexis Nexis and socialite Paris Hilton's T-Mobile cellular phone account, according to reports. According to the US Court, the number of young hackers is on the rise, and only about 1% of them get arrested.

In the case at hand, the judge sentenced the defendant to 11 months in a juvenile facility. He would have faced three counts of making bomb threats against a person or property as an adult, three counts of causing damage to a protected computer system as an adult, two counts of wire fraud, one count of aggravated identity theft, and one count of obtaining information from a protected computer in furtherance of a criminal act if he had been charged as an adult. This is definitely a departure from established criminal law standards.

2. **Organized hacktivists:** Hacktivists are hackers who have a specific (usually political) goal in mind. In other circumstances, the cause could be social activity, religious activism, or something else else. Attacks by a group of hackers known as the Pakistani Cyber Warriors on roughly 200 famous Indian websites are a good illustration of political hacktivists at action.

3. **Disgruntled employees:** It's hard to believe how vengeful disgruntled employees can be. They had the option of going on strike against their bosses up until now. Disgruntled employees can now cause more harm to their employers by committing computer-related crimes, which can bring entire systems down, thanks to increased computer independence and process automation.

4. **Professional hackers (Corporate espionage):** Business firms now save all of their information in electronic form as a result of extensive computerization. Hackers are used by rival firms to obtain industrial secrets and other information that could be useful to them. The temptation to hire professional hackers for industrial espionage derives from the fact that physical presence is no longer required to gain access to critical papers if hacking can retrieve them.

CRIMINAL LAW – GENERAL PRINCIPLES:

Certain people are exempt from criminal accountability for their activities under criminal law if they were under the age of criminal responsibility at the time. After attaining the initial age, there may be several levels of accountability based on age and the claimed offence.

Governments pass laws designating certain activities as wrongful or criminal. Antisocial behaviour can be stigmatised in a more positive way to demonstrate society's displeasure by using the word criminal. In this context, the phrase "age of criminal responsibility" is commonly used in two ways:

1. The range of ages establishes a child's exemption from the adult system of prosecution and punishment as a definition of the method for dealing with accused offenders. Parallel to the adult criminal justice system, most states construct unique juvenile justice systems. When children commit what would be considered an adult offence, they are redirected into this system.

2. As a child's physical ability to commit a crime. As a result, youngsters are regarded incapable of doing certain sexual or other acts that require more mature abilities.

The age of majority, as defined by legislation, is the point at which a person becomes an adult. It is the chronological point at which children legally gain majority authority over their persons, actions, and decisions, effectively ending their parents' legal control and responsibility over and for them. However, in the cyber realm, it is impossible to apply standard criminal law principles to determine liability. According to statistics, the majority of offenders in the internet realm are under the age of majority. As a result, a new procedure for dealing with cyber criminals must be developed. In different situations, ethics and morality have different and complex interpretations. Immoral and unethical behaviour includes everything that is contrary to public policy, harms the public good, or threatens public tranquilly. Imperialism, colonialism, and apartheid, which were once hot topics, have given way to cybercrime, hacking, and 'cyber-ethics,' among other phrases.

Positive Aspects of the IT Act, 2000:

1. Prior to the enactment of the Information Technology Act of 2000, an e-mail was not recognised as an accepted legal form of communication or as evidence in a court of law under Indian law. However, the IT Act of 2000 transformed this issue by recognising the electronic format as a legal medium. The Information Technology Act of 2000 is, without a doubt, a step forward.

2. From a corporate standpoint, companies will be able to conduct electronic trade using the legal framework established by the IT Act of 2000. The expansion of internet commerce in India was stifled until the Indian Cyber Law took effect, owing to a lack of legal framework to oversee business transactions conducted online.

3. Businesses will be able to employ digital signatures to complete online transactions. The IT Act of 2000 has given these digital signatures legal validity and authority.

4. In today's world, organisations save information on their own computer systems and keep a backup. Companies will now have a legislative recourse under the IT Act of 2000 if someone breaches into their computer systems or networks and causes harm or copies data. The remedy given under the IT Act, 2000 is in the form of monetary damages in the amount of Rs. 1,00,000 in compensation.

5. The Information Technology Act of 2000 defines a variety of cybercrimes, including hacking and computer code destruction. Prior to the implementation of the Indian Cyber Law, businesses were helpless because there was no legal recourse for such problems. The IT Act of 2000, on the other hand, completely transforms the landscape.

THE GREY AREAS OF THE IT ACT, 2000:

1. The IT Act, 2000 is likely to cause a conflict of jurisdiction.

2. Domain names are the foundation of electronic commerce. The Information Technology Act of 2000 makes no mention of domain names. Even domain names have not been defined, and domain name owners' rights and obligations are not mentioned in the legislation.

3. The Information Technology Act of 2000 does not address any issues relating to the protection of intellectual property rights in the internet environment. The law has left several gaps by leaving contentious but crucial topics such as internet copyrights, trademarks, and patents unaddressed.

4. As the cyber law evolves, new forms and manifestations of cybercrime emerge. The list of offences outlined under the IT Act of 2000 is far from exhaustive. However, the relevant provisions of the IT Act, 2000 are written in such a way that they appear to be the only cyber offences that are possible and exist. The Information Technology Act of 2000 does not cover a wide range of cybercrimes and Internet-related offences. These are some of them:
   a) Theft of Internet hours
   b) Cyber theft
   c) Cyber stalking
   d) Cyber harassment
   e) Cyber defamation
   f) Cyber fraud
   g) Misuse of credit card numbers
   h) Chat room abuse

5. The IT Act of 2000 fails to address a number of critical e-commerce issues, such as privacy and content control, to name a few. The topic of privacy has been completely ignored.

6. Another ambiguity in the IT Act is that it does not address any anti-trust issues.

7. The execution of the Indian Cyber Law is the most severe worry. The IT Act of 2000 does not include any guidelines for implementation. Furthermore, given India's poor internet penetration and the fact that most government and police employees are not computer knowledgeable, the new Indian cyber law raises more concerns than it solves. To remove the grey areas stated above, it appears that Parliament will need to alter the IT Act of 2000.

CONCLUSION:

The new laws, which can include all facets of cybercrime, should be passed in order to eliminate the law's murky areas. The recent bombings in Ahmedabad, Bangalore, and Delhi highlight the danger that cyberspace activities pose to humanity. Only technology, and its widespread application, I believe, can effectively combat challenges. The government should impose reasonable restrictions on the software that is readily available for download. The IT Act of 2000 should be updated to make it more efficient and effective in combating crime. Training and public awareness activities should be implemented in both private and public sectors. In India, the number of cyber cops should be expanded. The jurisdiction issue is present in the implementation phase, which should be resolved because cyber criminals have no jurisdiction limit, so why do the laws exist? After all, the laws are in place to punish the criminal, but the current situation allows them to flee.

Today's period necessitates the development of a "cyber-jurisprudence" on which "cyber-ethics" can be assessed and condemned. There is also a pressing need to develop a Cyber-Space code of ethics and discipline. When the country

was dealing with an increase in cybercrime, the Information Technology Act of 2000 was passed. Because the Internet is a conduit for vast amounts of data and a vast network of connections around the world, it is vital to exercise caution when using it. As a result, it is critical to educate everyone and practise safe computing in order to prevent cybercrime.

Many other hackers, like Frank William Abagnale and Robert Morris, want to put their hacking abilities to greater use. This practise is still going on today, with firms hiring smart hackers as security experts. There is also a pressing need to develop a Cyber-Space code of ethics and discipline. It is impossible to determine responsibility in cyberspace using standard criminal law criteria. Because the majority of cyber criminals are under the age of majority, a new legal structure to deal with them must be developed. Because the cyber world has no limits, enacting regulations that encompass all aspects is a Herculean undertaking. However, a balance must be maintained, and regulations must be developed to combat cybercrime.

REFERENCES:

1. Cybercrimes and Real World Society by Lalitha Sridhar.
2. Cyber Law and Information Technology by Talwanth Singh Addl.Distt. And Sessions Judge, Delhi.
3. www.gahtan.com/cyberlaw - cyber law encyclopedia.
4. www.legalserviceindia.com/cyber-crimes.
5. www.indlii.org/Cyberlaw.aspx
6. www.cybercases.blogspot.com
7. Information Technology Act, 2000